Mº DE LA PRESIDENCIA: gestión de la ciberseguridad en los servicios críticos asociados a Internet

El Ministerio de la Presidencia, derivado de la responsabilidad de garantizar la disponibilidad de los servicios críticos que presta de cara a Internet, incluyendo páginas web, servicio de correo electrónico y accesos remotos, puso en marcha un ambicioso proyecto de Ciberseguridad con un planteamiento de máximos para alcanzar unas altas cotas de protección mediante una combinación de servicios y plataformas de última generación. Para ello, contrató los servicios de la compañía española Grupo ICA, y en particular, el área de Ciberseguridad, que desde el principio colaboró en el análisis y diseño de la mejor solución, permitiendo la evolución continua de la misma para adaptarse a los cambios de escenario en el ámbito de la seguridad tecnológica.

Julián Hernández Vigliano / Fernando Quintanar Cenjor

Objetivo del Ministerio de la Presidencia

Dentro de las estrategias de ciberseguridad emprendidas por el Ministerio de la Presidencia, destaca la implantación de un servicio de seguridad gestionada (SOC) 24x7 de monitorización, operación y administración de las infraestructuras TI sobre los cuales se encuentran desplegados los principales servicios y aplicativos que el Ministerio de la Presidencia (MPR) tiene accesibles a través de Internet (en adelante servicios Internet).

Desde el punto de vista estratégico supone un cambio de paradigma en la gestión de la seguridad, pasando de un escenario reactivo a uno proactivo y preventivo. Para ello, MPR y el CiberSOC de ICA combinan sus conocimientos y experiencia para orientar el servicio a la detección proactiva de incidentes de seguridad, a partir de la monitorización de la infraestructura tecnológica completa, que suministrarán *logs* y otros flujos de información a la plataforma LogICA NG-SIEM.

Se establece asimismo un modelo de análisis de amenazas en tiempo real, capaz de detectar mediante la correlación de información proveniente de los sistemas internos del cliente y de la información extraída del servicio CiberSOC CiberInteligencia (analítica de información de internet, deep web y dark web) intentos de ataques por parte de grupos organizados, exfiltración de información, manejo de datos sensibles, análisis de información corporativa, analítica de vulnerabilidades y exploits asociados, seguimiento de actores así como mitigación de ataques en países extranjeros (bloqueo de IPs, dominios concretos, etc.).

Adicionalmente y para completar este requisito de proactividad y reactividad, se impulsó la implantación de un servicio de auditoría periódica, tanto externa como interna, confiando en los servicios del CiberSOC Atalaya y Achilles, que combinan las capacidades de plataformas con los conocimientos y experiencia del equipo Red Team del CiberSOC de Grupo ICA. Estas auditorías están orientadas a la detección temprana de vulnerabilidades, errores de configuración o situaciones que puedan derivar en una degradación del servicio. Por ello, se incluyen análisis de vulnerabilidades y test de intrusión, con idea de identificar y subsanar posibles debilidades en la arquitectura de seguridad (incluyendo plataforma de sistemas, redes y aplicaciones), evitando su explotación malintencionada y procediendo a su reconfiguración y subsanación.

Desde el punto de vista técnico, implica la construcción de un servicio amparado

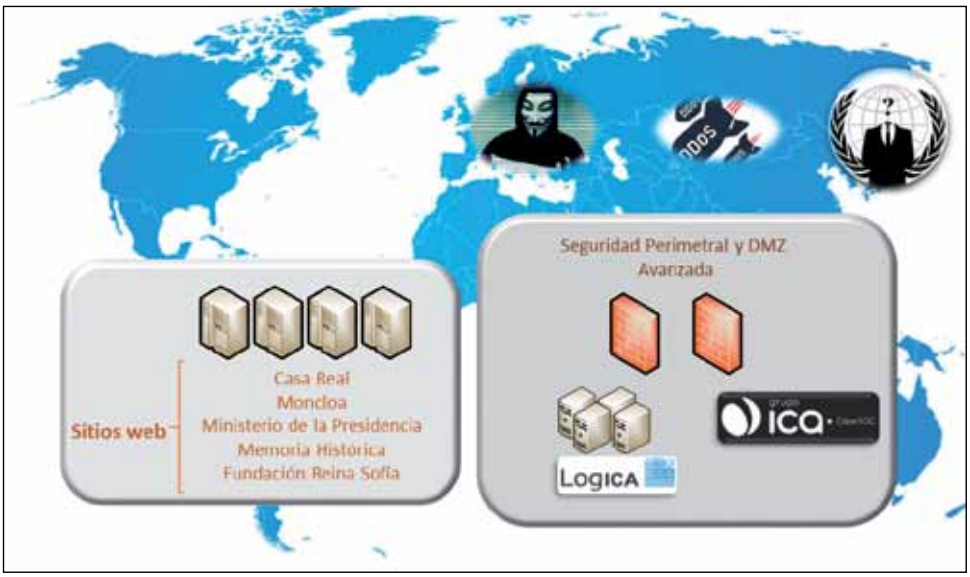

Figura 1

Dentro de las estrategias de ciberseguridad emprendidas por el Ministerio de la Presidencia, destaca la implantación de un servicio de seguridad gestionada (SOC) 24x7 de monitorización, operación y administración de las infraestructuras TI sobre los cuales se encuentran desplegados los principales servicios y aplicativos que el MPR tiene accesibles a través de Internet.

en las tecnologías más punteras del mercado de la seguridad y sustentado en personal con una cualificación técnica capaz de desarrollar las actividades con los máximos requisitos de seguridad y calidad.

Asimismo, y dada la criticidad de los activos y servicios a proteger, se trabaja en una modalidad mixta, con soporte *in situ* mediante un especialista en seguridad TI perteneciente al CiberSOC en modalidad 8x5 y el soporte remoto del personal completo de CiberSOC en modalidad 24x7. De manera adicional, se plantea un soporte basado en guardias para hacer frente a situaciones críticas puntuales, que requieren un soporte *in situ* mayor.

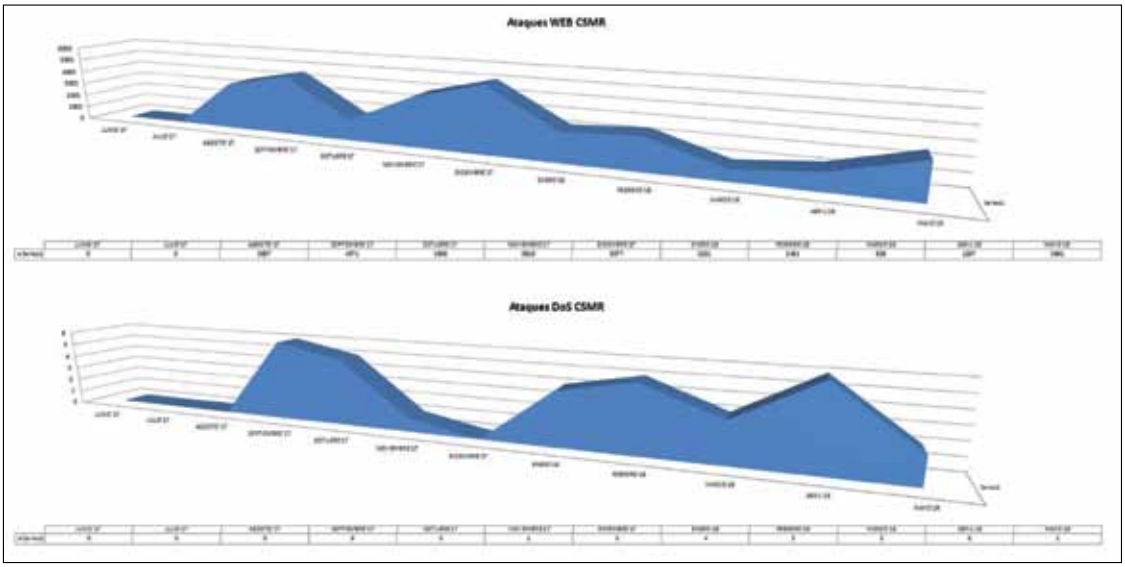

Figura 2

Dada la criticidad de los activos y servicios a proteger, se trabaja en una modalidad mixta, con soporte in situ mediante un especialista en seguridad TI perteneciente al CiberSOC en modalidad 8x5 y el soporte remoto del personal completo de CiberSOC en modalidad 24x7. De manera adicional, se plantea un soporte basado en guardias para hacer frente a situaciones críticas puntuales, que requieren un soporte in situ mayor.

Este servicio ha aportado una base de trabajo conjunto cliente-prestador, afrontando las diferentes situaciones de manera proactiva. A modo de ejemplo, en la **Figura 1** se muestra en modo gráfico el sumatorio de ataques contra las webs y posteriormente el Top 15 de ataques detectados (en ambos casos son sumatorios de las webs www.casareal.es y www.fundacionreinasofia.es).

Con estos requisitos, ICA elaboró una oferta de servicios basado en cuatro componentes esenciales:

- Servicio de monitorización de la plataforma TI.
- Servicio de operación y administración.
- Servicio de cibervigilancia.
- Servicio de análisis de vulnerabilidades y auditorías de seguridad.

Para ello, se articulan los siguientes servicios desde el CiberSOC de excelencia de Grupo ICA:

- LogICA Security Analytics: Detecta, contiene y mitiga las más sofisticadas ciberamenazas en tiempo real. Soportado por la plataforma NextGeneration SIEM LogICA.
- LogICA Cibervigilancia: Servicio personalizado de ciber alertas y amenazas para la prevención y detección de incidentes en tiempo real.
- LogICA Atalaya: Servicio de auditoría externa que permite identificar y gestionar vulnerabilidades encontradas desde el perímetro de la organización.
- LogICA Achilles: Servicio de gestión de vulnerabilidades y alerta temprana de red interna. ■

Julián Hernández Vigliano
Subdirector Adjunto
Subdirección General de Tecnologías
y Servicios de Información (EA0014593)
MINISTERIO DE LA PRESIDENCIA

Fernando Quintanar Cenjor
Director de la Unidad de Ciberseguridad
Grupo ICA